PUBLICATION

Protecting LTC Residents' PHI: Eight Tips for Avoiding a Data Breach

Authors: Layna S. Cook Rush
April 19, 2019

Organizations that meet the definition of "covered entity" under the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (HIPAA) must be diligent to maintain the privacy and security of residents' protected health information (PHI), but even organizations that do not fall under the purview of HIPAA may still be subject to state and federal laws that require the organization to maintain the privacy and security of residents' personal information. Moreover, the failure to adequately safeguard personal information could result in civil liability if residents seek judicial redress of an unauthorized disclosure or a security incident.

As such, organizations that maintain PHI or personal information should have in place policies and safeguards to protect against threats to the privacy and security of that information.

The following are considerations that may protect against an unauthorized disclosure of residents' personal information or a security incident that compromises that information:

1. **Update Business Associate Agreements routinely.** The Privacy Rule requires Covered Entities to enter into Business Associate Agreements with persons or organizations who perform certain functions or activities on behalf of, or provide certain services to, the Covered Entity that involve the use or disclosure of PHI. Business Associate Agreements should be routinely reviewed to determine if the agreement complies with the law and to determine if the agreement accurately describes the relationship between the Covered Entity and Business Associate. If the underlying relationship between the parties has changed or the manner in which the Business Associate will use or disclose PHI, the Business Associate Agreement should be revised to reflect that change.

2. **Conduct and review risk assessments.** The Security Rule requires Covered Entities to conduct a risk analysis to evaluate the likelihood of potential risks to electronic PHI (e-PHI) and to implement appropriate security measures to address the risk identified in the risk analysis. Even those organizations which are not subject to HIPAA but which use or maintain residents' personal information should still conduct a risk assessment to identify vulnerabilities, the likelihood of an occurrence and the potential impact of that occurrence. An organization cannot adequately guard against potential risk if it does not assess those risks. Risk assessments should be reviewed on an annual basis and any time that there has been a change in processes that could impact electronic information.

3. **Beware of phishing attacks.** A phishing attack is a fraudulent attempt to obtain sensitive information such as usernames and passwords by disguising as a trustworthy entity in an electronic communication. Phishing emails are one of the primary ways that bad actors access an organization's data. Employees should be trained to recognize phishing emails and should be made aware of the organization's process for reporting suspicious emails.

4. **Develop rules for use of portable devices.** Another way that the organization's information may be compromised is by lost or stolen equipment or data. From January 1, 2018 through August 31, 2018,

the Office of Civil Rights received reports of 192 theft cases affecting more than two million individuals. Organizations should implement device controls such as inventory of equipment and password requirements to guard against loss or theft of data, and simple policies, such as prohibiting employees from leaving devices in plain sight in a vehicle Organizations should also consider encrypting portable devices, which will protect information should there be a loss or theft of a device.

5. **Enforce password restrictions.** Even if an organization does not encrypt its portable devices, it can update a level of protection by instituting "strong" password requirements. For example, an organization can implement a policy that the password must be at least eight characters in length and alphanumeric. Additional protections include requiring that passwords be changed every 90 days and that forgotten passwords be replaced, not reissued. Employees should also be cautioned regarding sharing or publically posting passwords.

6. **Train employees.** Organizations should routinely train employees on the organization's policies and procedures for safeguarding PHI and personal information. In addition to annual training, organizations should consider periodic reminders, particularly regarding the organization's most substantial risks.

7. **Enforce sanctions.** The HIPAA Privacy Rule requires Covered Entities to have a policy addressing sanctions for the unauthorized use or disclosure of PHI. All organizations that maintain PHI or personal information should have a sanctions policy that sets forth the repercussions for violating the organization's privacy and security policies. And it is not enough to simply have a policy; the sanctions policy should be enforced to foster a culture of compliance.

8. **Get cyber insurance.** In 2018, the average total cost of a security breach was $3.86 million. Even small incidents involving one thousand compromised records cost between $52,000 and $87,000. It has been reported that 62 percent of small businesses go out of business within six months of a successful cyber-attack. Cyber insurance can help defray the cost of a breach and potentially save an organization from financial ruin. It is strongly recommended that organizations assess their potential liability and obtain insurance with adequate limits.

For more information on how your organization can assess and address its risks, contact the author, Layna Rush, or any member of Baker Donelson's Health Law Group.